PATENT ABSTRACTS OF JAPAN

(11)Publication number : 2000-338868

(43)Date of publication of application : 08.12.2000

(51)Int.Cl. G09C 1/00
H04L 9/08
H04L 9/10
H04L 9/32

(21)Application number : 11-146311

(22)Date of filing : 26.05.1999

(71)Applicant : NTT DATA CORP

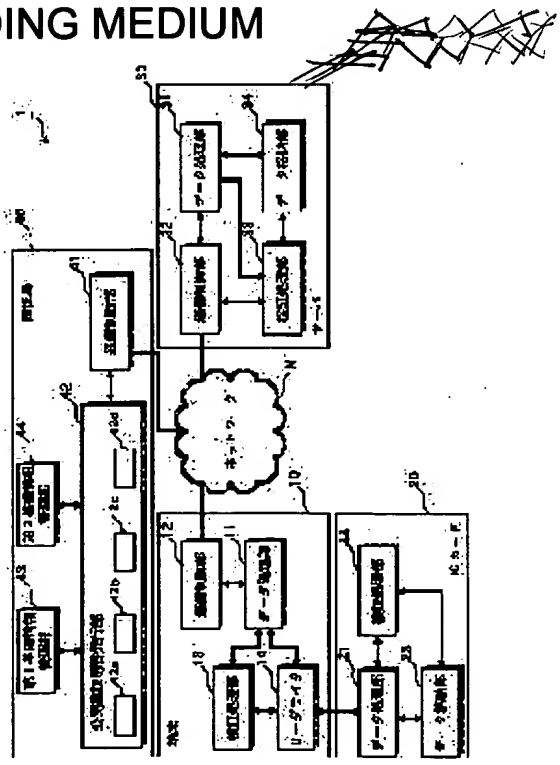
(72)Inventor : TAKAHASHI
YOSHIO
TSUCHIYA
SHIGEKI

(54) METHOD FOR ISSUING PUBLIC KEY CERTIFICATE, METHOD FOR VERIFYING, SYSTEM AND RECORDING MEDIUM

(57)Abstract:

PROBLEM TO BE SOLVED: To obtain a system which can issue and verify a public key certificate capable of dealing with to a plurality of formats.

SOLUTION: A verification office 40 generates signature data for EMV use objecting fundamental information for the EMV use when receiving information applying an issue of a public key



certificate. Also, it generates the signature data for X 509 use objecting information containing the fundamental information for the EMV use and the signature data for the EMV use. It issues the X 509 public key certificate containing all of the generated information and data. This X 509 public key certificate is converted into the EMV public key certificate at a terminal 10 in order to be able to use with an IC card 20.

LEGAL STATUS

[Date of request for examination]	08.11.2000
[Date of sending the examiner's decision of rejection]	
[Kind of final disposal of application other than the examiner's decision of rejection or application converted registration]	
[Date of final disposal for application]	
[Patent number]	3617789
[Date of registration]	19.11.2004
[Number of appeal against examiner's decision of rejection]	
[Date of requesting appeal against examiner's decision of rejection]	
[Date of extinction of right]	

DERWENT-ACC-NO: 2001-116262

DERWENT-WEEK: 200511

TITLE: Disclosure **key certificate issue procedure involves generating disclosure key certificate** of certain formats from relative signature data and basic information generated based on certificate of other format

---

Basic Abstract Text - ABTX (1):

NOVELTY - Signature data and basic information for a format are used for **generating disclosure key certificate,** based on specific application. The disclosure **key certificate generated for one format is used for generating** signature data and basic information for other formats which are inturn used for generating disclosure by certificates for other formats.

Basic Abstract Text - ABTX (5):

USE - For issuing disclosure key certificate for use in **IC cards** for electronic mail system, electronic amount settlement system, electronic commercial transaction system and electronic application system.

Basic Abstract Text - ABTX (6):

ADVANTAGE - Waste of resources in **IC card** for disclosure key certificate is prevented, as disclosure key certificate of corresponding format is published.

Title - TIX (1):

Disclosure **key certificate issue procedure involves generating disclosure key certificate** of certain formats from relative signature data and basic information generated based on certificate of other format

* NOTICES *

1.This document has been translated by computer. So the translation may not reflect the original precisely.
2.**** shows the word which can not be translated.
3.In the drawings, any words are not translated.

DETAILED DESCRIPTION

[Detailed Description of the Invention]
[0001]
[Field of the Invention] This invention relates to the technique of publishing the public key certificate which can respond to both a format of the general-purpose criterion for media, and the original format suitable for the small media of a resource, and the verification technique of the published public key certificate. It is information processing means to use a public key certificate (a terminal, IC card, etc.), and media mean the specification of a public key certificate that media can interpret a format.
[Detailed description]
[0002]
[Background of the Invention] In recent years, various systems using networks, such as an electronic mail system, a cybermoney system, an electronic clearing system, an electronic commerce system, and an electronic application system, are put in practical use. Although encoding technology is applied in such a system since communicative secrecy nature becomes very important, a public key cryptosystem with the advantage of the effort of current which is in charge of maintaining a cryptographic key and a decode key being small, and ending is used widely.
[0003] In a public key cryptosystem, in order to prove the owner of the public key, it is common that the engine called the strong certificate authority of public responsibility publishes the public key certificate of entering signature data by the certificate authority. Although corresponding to a public key certificate flexibly to various purposes and applications is called for on the property, it has secured the versatility by including various items in the format conventionally. For example, "X509" of ITU-T (International

Telecommunications Union telecommunication standardization section) which is the criterion of a public key certificate includes very many items, and is quite complicated [the contents]. Such a complicated public key certificate of the contents is the versatility, therefore very attractive thing, but on the other hand when applying this to what has few resources, such as an IC card, it has a difficulty.

[0004] That is, in the small IC card of a resource, in order to deal with the above common high public key certificates of versatility, problems, such as increase of a program size, an increment in the processing time, and pressure of memory, occur, and the case where it cannot use as it is arises. In such a case, although it is necessary to build exclusive infrastructures other than the infrastructure for flexible public key certificates for that purpose although it is possible to adopt an original format of specific service limitation, this is seen from the time and effort and field of cost, and cannot necessarily say it as an appropriate solution means.

[0005] When a high format of versatility, such as ITU-T "X509", is adopted as the small thing of resources, such as an IC card, Or although a theory top can cancel the above difficulties when to change a general-purpose format into an original format inside an IC card, and to keep this is decided The resource with which the IC card was restricted will be consumed in order to realize an interpretation and conversion function of a format, and the situation where the function which could not mount primarily or it was originally going to attain cannot fully be attained arises.

[0006] This invention makes it the main technical problem to offer the issue approach of the high public key certificate of versatility which could respond also to the standard format and also fitted use by the small media of a resource, issue equipment, and an issue system. This invention makes it the technical problem to offer the record medium which becomes suitable when realizing the verification approach that a public key certificate is appropriately verifiable, and the issue approach of a public key certificate, on a general-purpose computer again.

[0007]

[Means for Solving the Problem] This invention offers the issue approach of two kinds of public key certificates which are explained below, in order to solve the above-mentioned technical problem. While the issue approach of the 1st public key certificate generates the signature data for the format concerned of 1 for the basic intelligence for a format of one among two or more basic intelligence for public key certificates generated based on predetermined

application information The public key certificates for a format of above others including the signature data for a format of these these others for said basic intelligence and signature data which were generated, and the basic intelligence for other formats are drawn up. moreover, the basic intelligence for said format of the drawn-up public key certificate to 1 and the signature data for said format of 1 -- said -- others -- the basic intelligence for a format -- said -- others -- the signature data for a format are acquired and the public key certificate for said format of 1 is drawn up based on the information and signature data which were acquired. It is the issue approach of a public key certificate including such a process.

[0008] The public key certificate published by this approach is the following, and can be made and verified. Each basic intelligence and signature data are picked out from a public key certificate. First, when required The basic intelligence corresponding to a format is generated. picking appearance -- changing each basic intelligence into other formats other than the format to which it corresponds the bottom -- being concerned -- others -- When the basic intelligence taken out from the public key certificate or the basic intelligence corresponding to a format of above others, and either of two or more signature data picked out from the public key certificate agree, the public key certificate is judged to be just.

[0009] When a format is changed, it is usual that it becomes impossible to perform collating between basic intelligence and signature data. However, two or more signature data are contained in the public key certificate published by this invention, and since this signature data is generated considering the basic intelligence changed into other formats as a candidate for a signature, collating becomes possible after format conversion. Even if it adopts a format of the basic intelligence optimized to specific service / application by being premised on format conversion, it becomes unnecessary moreover, to build the infrastructure only for original formats.

[0010] The activation is possible for the issue approach of the above-mentioned public key certificate by the public key certificate issue equipment or the system constituted as follows, for example. A basic intelligence generation means to classify into basic intelligence common to all formats, and each format two or more basic intelligence for the public key certificates with which public key certificate issue equipment was generated based on predetermined application information at the basic intelligence of a proper, It has a signature means to generate the signature data for the format concerned of 1 for the basic intelligence of a proper, in said common basic intelligence

and a format of 1. To the generated basic intelligence and signature data, and other formats, furthermore, the basic intelligence of a proper, It has an issue means to draw up the public key certificates for other formats including the signature data for a format of these these others for basic intelligence common to a format and other formats of 1. It is equipment which publishes the public key certificate which can respond to both a format of 1, and other formats.
[0011] A public key certificate issue system is constituted including the 1st equipment which publishes the public key certificate which can respond to a multiple format based on predetermined application information, and the 2nd equipment which changes the published public key certificate into the public key certificate of an original format. A basic intelligence generation means to classify into basic intelligence common to all formats, and each format two or more basic intelligence for the public key certificates with which the 1st equipment was generated based on application information at the basic intelligence of a proper, A signature means to generate the signature data for the format concerned of 1 for the basic intelligence of a proper to said common basic intelligence and a format of 1, The signature data for a format of these these others for basic intelligence common to the basic intelligence of a proper, a format of 1, and other formats are included in the basic intelligence and signature data which were generated, and other formats. The public key certificate for other formats It is what has a public key certificate issue means to create. The 2nd equipment From the public key certificate for other formats, to common basic intelligence and a format of 1 The basic intelligence of a proper, It has a means to draw up the public key certificate for a format of 1 based on the information and data which acquired the basic intelligence of a proper, and the signature data for other formats, and were acquired at the signature data for a format of 1, and other formats. After verifying the public key certificate for a format of 1, the 2nd equipment is constituted so that the public key certificate may be stored in a predetermined information record medium. In addition, the 1st equipment and the 2nd equipment may be independent equipment connected through the network, and may build one [at least] function of the 1st equipment and the 2nd equipment within the same information processor or a system. In the case of the latter, the public key certificate issue approach of this invention is realizable in the condition of having been concealed outside by using the information processor or system as proxy (proxy) equipment. Moreover, only the part which is not in the existing public key issue system is arranged to this proxy equipment, and operation of this invention becomes easier because it is made to publish a

public key certificate in collaboration with the existing public key issue system.

[0012] Next, the issue approach of the 2nd public key certificate is explained. While this approach arranges the basic intelligence of two or more formats for public key certificates generated based on predetermined application information in predetermined order The basic intelligence corresponding to [generate signature data for the connection hash value which connected each hash value of each basic intelligence, and] a format available at an applicant side, It is an approach including the process which draws up public key certificates including the hash value generated from the basic intelligence of other formats other than a format of this basic intelligence, and the generated signature data. Connection of a hash value is performed by judging the logic conditions of two or more hash values. As compared with the 1st public key certificate issue approach, the issue approach of the 2nd public key certificate can make small the amount of data of the public key certificate obtained by that cause. It is based on this having the amount of data of a hash value smaller than the amount of data of signature data.

[0013] Verification of the public key certificate published by this issue approach is performed by [as being the following]. Namely, while hashing the process which picks out basic intelligence, two or more hash values, and signature data from a public key certificate, and the taken-out basic intelligence in the equipment which verifies and generating a hash value The process which connects the generated hash value and the hash value taken out from said public key certificate, and generates a connection hash value, The process which compares the generated connection hash value with the signature data picked out from said public key certificate is performed in this order, and when signature data and a connection hash value agree, a public key certificate is judged to be just.

[0014] The issue approach of the 2nd public key certificate can be enforced, for example in the following public key certificate issue equipments. A basic intelligence array means to arrange the basic intelligence of two or more formats for the public key certificates with which this public key certificate issue equipment was generated based on predetermined application information in predetermined order, A signature means to generate signature data for the connection hash value which connected each hash value of two or more basic intelligence, It has an issue means to draw up public key certificates including the hash value and the generated signature data generated from basic intelligence other than the basic intelligence

corresponding to an available format, and the basic intelligence corresponding to this format by the applicant side. It is characterized by publishing one public key certificate which can respond to two or more formats.

[0015] The record medium used when performing the issue approach of the 1st and 2nd public key certificates on a general-purpose computer is as follows respectively. The record medium for realizing the issue approach of the 1st public key certificate on a computer is a record medium with which the program for performing the following processing was recorded on the computer and in which a computer readout is possible.

(1-1) The processing which prepares two or more basic intelligence for public key certificates based on predetermined application information, Basic intelligence and signature data which generate the signature data for the format concerned of 1 for the basic intelligence for a format of one among said two or more basic intelligence and which were processed and generated (1-3), (1-2) Processing which draws up the public key certificates for other formats including the signature data for a format of these these others for the basic intelligence for other formats.

[0016] The record medium for realizing the issue approach of the 2nd public key certificate on a computer is a record medium with which the program for performing the following processing was recorded on the computer and in which a computer readout is possible.

(2-1) The processing which generates the basic intelligence of two or more formats for public key certificates based on predetermined application information, The processing of the basic intelligence of two or more formats which generates a hash value respectively, (2-2) The basic intelligence corresponding to the processing which generates signature data for the connection hash value which connected two or more generated hash values, and a format available at an applicant (2-4) side, (2-3) Processing which draws up public key certificates including the hash value generated from the basic intelligence of other formats other than a format of this basic intelligence, and said generated signature data.

[0017]

[Embodiment of the Invention] Hereafter, with reference to a drawing, the gestalt of operation of the public key certificate issue approach by this invention, the verification approach, and an issue system is explained. Here, the example of the public key certificate in which the transposition between ITU-T "X509 which is a standard format", and the simple format for the small IC cards of a resource "EMV" is possible is given.

[0018] (The 1st operation gestalt) The gestalt of operation of the 1st public key certificate issue approach is explained first. Drawing 1 is the block diagram of a public key certificate service system suitable for operation of this approach. This public key certificate service system 1 With the certificate authority 40 which has the function to publish the public key certificate which has the compatibility of a format, the terminal 10 which has the function to change the above-mentioned public key certificate into the public key certificate of an original format, and a terminal 10 While holding the public key certificate by which format conversion was carried out, the server 30 with the verification function of the public key certificate of IC card 20 and IC card 20 to have the verification function of the public key certificate of a server 30 is connected to the network N of the environment in which two-way communication is possible respectively, and it is constituted.

[0019] A terminal 10 is a kind of computer which has the reader writer 14 which delivers and receives information between IC cards 20. This terminal 10 is constituted including the data-processing section 11 formed when CPU of the computer which is not illustrated reads and executes a predetermined program under a self operating system, the communications control section 12, and the verification processing section 13. Between IC card 20 grades, the data-processing section 11 exchanges data, or performs format conversion of a public key certificate etc. according to a predetermined conversion algorithm, and the communications control section 12 controls information which goes via a network. The verification processing section 13 verifies a public key certificate etc.

[0020] IC card 20 is constituted including the data storage section 23 which stores the data-processing section 21 which exchanges data, the verification processing section 22 which performs verification of a public key certificate, the public key certificate of self, a public key [finishing / verification], etc. between terminal 10 grades. These data-processing sections 21, the verification processing section 22, and the data storage section 23 are formed when CPU performs the program in ROM which is not illustrated.

[0021] The server 30 is constituted including the data storage section 34 which stores the data-processing section 31 which exchanges data, the communications control section 32 which controls the information from Network N, the verification processing section 33 which performs verification of a public key certificate, the verified public key certificate, a public key, etc. between the terminal 10 or the certificate authority 40.

[0022] A certificate authority 40 is what is realized according to a computer

thru/or a computer system. Various functional block formed when CPUs, such as a computer, read and execute a predetermined program under a self operating system, That is, it is constituted including the communications control section 41 which controls the information from Network N, the public key certificate issue section 42 which manages issue and generation of a public key certificate, the 1st basic intelligence Management Department 43 which manages the basic intelligence of a respectively different format, and the 2nd basic intelligence Management Department 44. The public key certificate issue section 42 contains basic intelligence generation section 42a which generates the basic intelligence for public key certificates based on the application information from an applicant, signature section 42b which generates the signature data for basic intelligence, and issue section 42c which draws up public key certificates including basic intelligence and signature data (issue).

[0023] Next, actuation of the public key certificate service system constituted as mentioned above is explained. First, the procedure in the case of publishing a public key certificate in a certificate authority 40 is explained with reference to drawing 2 . Here, the public key certificate of the X509 format in consideration of being changed into the EMV format for IC card 20 later shall be published. In future explanation, when the class of format needs to be distinguished, X509 format is expressed as "X509", and an EMV format is expressed as "EMV." Moreover, an item required only for A and EMV is set [an item common to X509 and EMV among the items which should be described in the public key certificate of each format] to B for C and an item required only for X509.

[0024] When the application information on a public key certificate is received from a terminal 10 (step S101), the public key certificate issue section 42 of a certificate authority 40 creates thru/or classifies the item (A, B, C) corresponding to X509 and EMV based on this application information, and makes the 2nd basic intelligence Management Department 44 generate signature data SIGN#2 for EMV for Item C and Item B (step S102). The public key certificate issue section 42 makes the 1st basic intelligence Management Department 43 generate signature data SIGN#1 Item C, Item A, and for X509 for extended data APDX#2 again as data ("extended data") APDX#2 which store Item B and the above-mentioned signature data SIGN#2 in the extended partition of a public key certificate (step S103).

[0025] Then, the X509 public-key certificate containing signature data SIGN#1 Item C, Item A, and for X509 is published (step S104), and this is

sent to a terminal 10 through the communications control section 41. Thus, the published X509 public-key certificate is changed into an EMV public key certificate at a terminal 10, in order to enable it to use it in IC card 20. Item C and Item B are acquired from a X509 public-key certificate, and, specifically, this is set to basic intelligence DATA#2 of EMV. Moreover, signature data SIGN#2 for EMV are acquired from extended data APDX#2, signature data SIGN#1 of further the for Item A and for X509 is acquired, and it changes into an EMV public key certificate. Thus, the changed EMV public key certificate can be changed now into a X509 public-key certificate by the terminal 10 or the server 30 at any time.

[0026] Drawing 3 is drawing having shown notionally the correspondence relation of the item of a X509 public-key certificate and an EMV public key certificate. The X509 public-key certificate published from the certificate authority 40 has the basic information field and the radical station name field, as shown in the drawing 3 left-hand side. Item C, Item A, and extended data (Item B and signature data SIGN#2) APDX#2 are stored in a basic information field. Such storing information is set to basic intelligence DATA#1 for X509, and signature data SIGN#1 for this basic intelligence DATA#1 is stored in a radical station name field.

[0027] On the other hand, as is shown in drawing right-hand side, Item C and Item B are stored in the basic information field, and these are set to basic intelligence DATA#2 for EMV by the EMV public key certificate. And signature data SIGN#2 for these basic intelligence DATA#2 are stored in a radical station name field. Signature data SIGN#1 Item A and for X509 is stored in the attached data area of an EMV public key certificate as attached data APDX#1.

[0028] Next, verification processing of each public key certificate is explained. Verification processing of a X509 public-key certificate is processing to which signature data SIGN#1 for X509 checks whether it is right signature data about basic intelligence DATA#1, and verification processing of an EMV public key certificate is processing which checks whether signature data SIGN#2 for EMV are right signature data about basic intelligence DATA#2.

[0029] Although it is usual that it becomes impossible to collate signature data when format conversion is performed Signature data SIGN#1 by two kinds of formats and SIGN#2 are contained in the public key certificate of this operation gestalt. And among these signature data, since the thing corresponding to one format is what was generated considering the basic

intelligence changed into the format of another side as a candidate for a signature, it becomes possible to perform collating etc. after format conversion. That is, if the signature data generated for the basic intelligence changed into the format use is expected to be are included in one of two or more of the signature data and the public key certificate is drawn up, it will become possible after format conversion to collate basic intelligence and the signature data created based on it.

[0030] Thus, the public key certificate published according to this operation gestalt has the advantage by which the structure of a system which it becomes unnecessary to build the infrastructure for every format separately, and uses a public key certificate since it can respond to both EMV formats which are easy to use in what has a small resource is simplified like X509 high format of versatility, and IC card 20.

[0031] Moreover, the big terminal 10 of a resource performs verification processing of a public key certificate in which format conversion is required, it is storing in IC card 20 the public key certificate with which justification's was checked, and it becomes, without using vainly the resource restricted by the IC card 20 side for format conversion.

[0032] As mentioned above, although issue of the public key certificate which can respond to both X509 format and an EMV format, and the example of verification were shown, it is also possible to enable it to correspond to three or more kinds of formats with one public key certificate. For example, drawing 4 is the conceptual diagram of the public key certificate which enabled it to correspond to four kinds of formats (format #1, format #2, format #3, format #4). The big workstation of a resource performs bidirectional format conversion from basic intelligence DATA#1 to basic intelligence DATA#4, and only verification which does not require the contents check or format conversion of a format is performed in the small IC card of a resource.

[0033] When making it correspond to four kinds of formats like drawing 4 , a total of four-piece (SIGN#1, SIGN#2, SIGN3, SIGN4) creation of one certain format, for example, the signature data generated about the basic intelligence (DATA#2, DATA#3, DATA#4) which changed basic intelligence DATA#1 in format #1 and this basic intelligence DATA#1 into other formats, is carried out.

[0034] In addition, in case the signature data about one format are generated, there is the approach of bending as the approach of making it applicable to a signature also including the signature data generated in other formats. The former approach is the approach of creating signature data SIGN#1 in the

example of format #1 of drawing 4 for [other than basic intelligence DATA#1] other signature data SIGN#2, SIGN#3, and SIGN#4, and the latter approach is the approach of generating signature data SIGN#1 by making only basic intelligence DATA#1 applicable to a signature.

[0035] The basic intelligence field of a public key certificate is made read according to the predetermined format conversion Ruhr, when making it read into an IC card since it is expressed by either of four patterns after changing into a required format. For example, the basic intelligence of a public key certificate is DATA#1 expressed by format #1, and when verifying by format #2 in an IC card, it checks that the signature data in basic intelligence DATA#2 which changed basic intelligence DATA#1 into format #2 are signature data SIGN#2 corresponding to it. It is the same also in case it changes into the format of those other than format #2.

[0036] (The 2nd operation gestalt) Next, the gestalt of implementation of the issue approach of the 2nd public key certificate is explained. The system configuration for enforcing this approach is the same as that of the public key certificate service system shown in drawing 1 almost. However, as for the public key certificate service system of this operation gestalt, the configuration of a certificate authority differs from the thing of the service system 1 of the 1st operation gestalt. The certificate authority 400 of this operation gestalt has the communications control section 410, the public key certificate issue section 420, and the signature section 430 as it was shown in drawing 5 .

[0037] Basic intelligence generation section 420a to which the public key certificate issue section 420 generates the basic intelligence corresponding to two or more formats based on the application information on public key certificate issue, Hash section 420b which hashes each of the generated basic intelligence and generates two or more hash values, It consists of applicants including issue section 420c which draws up public key certificates including all the hash values and the above-mentioned signature data which were generated from basic intelligence other than the basic intelligence corresponding to an available format, and this basic intelligence (issue).

[0038] First, in this certificate authority 400, the actuation in the case of publishing a public key certificate with the compatibility of X509 and EMV like the 1st operation gestalt is explained. With this operation gestalt, basic intelligence expressed by DATA#1 and EMV (format #2) in the basic intelligence expressed by X509 (format #1) is set to DATA#2. [0039] Basic intelligence DATA#1 uses the item B required only for EMV as the extended

data which are another field, is arranged in order of Item C, Item A, and Item B, and is built. C is a common item. By using the item A required only for X509 as the attached data which are another field, basic intelligence DATA#2 are arranged in order of Item C, Item B, and Item A, and they are built.
[0040] First, on the other hand, h (x) is made into a tropism Hash Function, and a certificate authority 400 defines hash value H1=h (C, A) and hash value H2=h (C, B). And the radical station name data of a certificate authority 400 are generated by making applicable to a signature the connection hash value which connected these two hash values H1 and H2. And the X509 public-key certificate containing basic intelligence DATA#1, a hash value H2, and radical station name data is published. About an EMV public key certificate, it publishes as a thing containing basic intelligence DATA#2, a hash value H1, and radical station name data.
[0041] Specifically, issue of a public key certificate is made by the procedure as shown in the flow chart of drawing 6 . That is, if the application information on public key certificate issue is received from a terminal 10 (step S201), while the public key certificate issue section 42 generates the item (A, B, C) corresponding to each format, it will ask for hash value H1=h (C, A) and H2=h (C, B) using Hash Function h (x) (step S202).
[0042] Next, the signature data SIGN are generated for the connection hash value (H1|H2) which connected the hash value H1 and the hash value H2 (step S203). The public key certificate issue section 42 uses Item C and Item A as extended data, publishes the X509 public-key certificate containing Item B, a hash value H2, and radical station name data again (step S204), and sends this to a terminal 10 through the communications control section 410.
[0043] When changing this X509 public-key certificate into an EMV public key certificate, {C, B, A}, and a hash value H1 are changed into h (C, A) for basic intelligence DATA#2 of EMV. On the other hand, when changing an EMV public key certificate into a X509 public-key certificate, {C, A, B}, and a hash value H2 are changed into h (C, A) for basic intelligence DATA#1 of X509.
[0044] In the case of X509, verification processing of each public key certificate calculates a hash value H1 from Item C and Item A, and carries out by checking whether the radical station name data SIGN are right signature data about a connection hash value (H1|H2). On the other hand, in EMV, a hash value H2 is calculated from Item C and Item B, and it performs it by checking whether the radical station name data SIGN are right signature data about a connection hash value (H1|H2). [0045] Next, the example of the

public key certificate which enabled it to correspond to four kinds of formats (format #1, format #2, format #3, format #4) as well as the case of the 1st operation gestalt is explained. Drawing 7 is the conceptual diagram of the format conversion by this operation gestalt.

[0046] First, three hash values which searched for the basic intelligence (DATA#2, DATA#3, DATA#4) expressed in basic intelligence DATA#1 of format #1, and other three formats by the Hash Function (HASH#2, HASH#3, HASH#4), One radical station name data (SIGN) which generated the connection hash value which connected these three hash values as a candidate for a signature is prepared. Like the case of the 1st operation gestalt, since it is expressed by four ones of patterns, when making the basic intelligence field of a public key certificate read into IC card 20, it is possible to make it read according to the format conversion Ruhr, after changing into a required format.

[0047] Conversion of a format can be performed as follows. For example, the case where it changes into format #2 from format #1 is considered. In this case, hash value HASH#1 [of format #1] of basic intelligence DATA#1 is made first. Next, basic intelligence DATA#1 is changed and basic intelligence DATA#2 of format #2 are made. Since hash value HASH#2 before conversion become unnecessary, it throws away. Although it is not necessary to throw away when allowances are in a storage region, it needs to be checked that basic intelligence DATA#2 and hash value HASH#2 have consistency. When verifying format #2, basic intelligence DATA#2 are hashed, hash value HASH#2 are calculated, the radical station name data SIGN are generated by making applicable to a signature what connected from HASH#1 to HASH#4, and it checks whether it is right signature data.

[0048] Since each hash value is reproducible at any time if the format conversion of the basic intelligence in each format can be carried out, in devices, such as an IC card, after verification processing does not need to save them and can lessen a storage region. for example, illustration -- like -- the case of format #2 -- after verification processing -- each -- hash value HASH#1, HASH#3, and HASH#4 can be thrown away In this case, in case it changes into other formats, format conversion will be carried out to sequence to format #1- format #4, and HASH#1-HASH#4 will be reproduced.

[0049] By the issue approach of the public key certificate by this operation gestalt, one radical station name data and three hash values are needed to the signature data the number of the 1st operation gestalten is [data] four being needed. Usually, since signature data become quite larger than a hash value,

there is little amount of data which the direction of this operation gestalt saves, and it ends.

[0050] Moreover, although the example in case a certificate authority 40 is equipped with a new component and consists of a 1st operation gestalt and a 2nd operation gestalt was explained, an information processor thru/or a system with the function of the certificate authority 40,400 of each operation gestalt may be arranged on Network N, and the above-mentioned function thru/or processing may be realized through this information processor thru/or system. A public key certificate can be published now in the condition of having been concealed from the outside with constituting an information processor thru/or a system from a proxy server especially.

[0051]

[Example] Next, the example of this invention is explained. When passing against each public key when just, and enabling it to perform cryptocommunication, drawing 8 is a sequence chart while verifying a public key certificate mutually through a terminal 10 between a server 30 and IC card 20. In drawing 8 , a X509 public-key certificate for a public key certificate for EMV-CERT#1 to prove the justification of public key #1 which IC card 20 holds, and X509-CERT#1 to prove an available X509 public-key certificate and the justification of public key #2 in which a server 30 holds X509-CERT#2 in a terminal 10, and EMV-CERT#2 are the EMV public key certificates which changed X509-CERT#2.

[0052] The user who holds IC card 20 equips the reader writer 14 of a terminal 10 with the IC card 20. If equipped with IC card 20, a terminal 10 will receive EMV-CERT#1 (the basic intelligence field is generated in the format of EMV) from IC card 20, and will change this into X509-CERT#1 in the data-processing section 11 (T301). Then, verification processing of X509-CERT#1 is performed in the verification processing section 13 (T302), and when it can be judged that the X509-CERT#1 is just, public key #1 is stored (T303). The data-processing section 11 transmits a verification terminate signal to IC card 20 through the reader writer 14. If a terminal 10 receives the demand which transmits X509-CERT#1 to a server 30 from IC card 20 again, a terminal 10 will send X509-CERT#1 to a server 30.

[0053] The server 30 which received X509-CERT#1 performs verification processing of X509-CERT#1 in the verification processing section 33 (S301). When it can be judged that it is just, public key #1 is stored in the data storage section 34 (S302). Moreover, X509-CERT#2 stored in the data storage section 34 are transmitted to addressing to terminal 10. The terminal 10 which

received X509-CERT#2 from the server 30 changes X509-CERT#2 into EMV-CERT#2 in the data-processing section 11 (T304), and sends this to IC card 20 through the reader writer 14.

[0054] IC card 20 which received EMV-CERT#2 stores public key #2 in the data storage section 23, when verification processing of EMV-CERT#2 is performed in the verification processing section 22 (I301) and it can be judged that it is just (I302).

[0055] Consequently, IC card 20 stores public key #2 of a server 30, and on the other hand, in case a server 30 will store public key #1 of IC card 20 and performs cryptocommunication mutually using these public keys, it can verify the data of the other party. In addition, it is desirable that the form which defines one standard format and goes via it defines the conversion Ruhr to the format according to individual on the occasion of conversion of a format. By doing in this way, also when the number of the formats according to individual increases, it can respond easily.

[0056]

[Effect of the Invention] Since resources, such as an IC card, become possible [adopting an available simple format also in a small device], adopting a high format of versatility in infrastructure construction since it becomes possible to use two or more formats according to the public key certificate of this invention so that clearly from the above explanation, duplication development of an infrastructure and waste of the resource by the public key certificate in an IC card etc. can be prevented.

[Translation done.]